A. KAWAMOTO
3/14/01
Q63597
1 of 1

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

CERTIFIED COPY OF PRIORITY DOCUMENT

出願年月日
Date of Application: ２０００年 ３月１５日

出願番号
Application Number: 特願２０００－０７３０６４

願人
Applicant (s): 日本電気株式会社

２００１年 １月２６日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２００１－３００１７４９

【書類名】　特許願
【整理番号】　37400189
【提出日】　平成12年 3月15日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 13/00
【発明の名称】　マルチキャストシステム、認証サーバ端末、マルチキャスト受信者端末管理方法、並びに記録媒体
【請求項の数】　9
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　川本　亜紀子
【特許出願人】
【識別番号】　000004237
【氏名又は名称】　日本電気株式会社
【代理人】
【識別番号】　100108578
【弁理士】
【氏名又は名称】　高橋　詔男
【代理人】
【識別番号】　100064908
【弁理士】
【氏名又は名称】　志賀　正武
【選任した代理人】
【識別番号】　100101465
【弁理士】
【氏名又は名称】　青山　正和
【選任した代理人】
【識別番号】　100108453
【弁理士】

【氏名又は名称】　村山　靖彦

【手数料の表示】

【予納台帳番号】　008707

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9709418

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　マルチキャストシステム、認証サーバ端末、マルチキャスト受信者端末管理方法、並びに記録媒体

【特許請求の範囲】

【請求項１】　マルチキャストにおける送信者端末と受信者端末の管理を行う認証サーバ処理装置と、

該認証サーバ処理装置に対するログインを行う第１のユーザ処理装置を有し、マルチキャストデータを送信する送信者端末と、

該認証サーバ処理装置に対するログインを行う第２のユーザ処理装置を有し、マルチキャストデータを受信する受信者端末と、

を備えるマルチキャストシステム。

【請求項２】　前記送信者端末はマルチキャストデータを送信する際に、第１のユーザ処理装置から前記認証サーバ処理装置に対してログイン要求を行い、前記認証サーバ処理装置からログインを許可されると、マルチキャストデータを暗号化して送信することを特徴とする請求項１に記載のマルチキャストシステム。

【請求項３】　前記受信者端末は予め前記認証サーバ処理装置に登録されており、マルチキャストデータを受信する際に、第２のユーザ処理装置から前記認証サーバ処理装置に対してログイン要求を行い、前記認証サーバ処理装置からログインを許可されると、前記認証サーバ処理装置から渡された暗号鍵を用いてマルチキャストデータを復号化してアプリケーションを受信することを特徴とする請求項１に記載のマルチキャストシステム。

【請求項４】　前記認証サーバ処理装置に登録していない前記受信者端末はマルチキャストデータを受信する際に、第２のユーザ処理装置から前記認証サーバ処理装置に対してログイン要求を行うが、前記認証サーバ処理装置からログイン不許可となり暗号鍵は渡されないことを特徴とする請求項１に記載のマルチキャストシステム。

【請求項５】　前記認証サーバ処理装置は定期的に暗号鍵を生成し、ログイン時と同様に暗号鍵を受信者端末へ配布し、定期的に配布する暗号鍵を該受信者

端末のユーザ処理装置が受け取らなかった場合は、前記認証サーバ処理装置にてログアウト処理を行うことを特徴とする請求項１又は請求項３に記載のマルチキャストシステム。

【請求項６】　前記受信者端末のアプリケーションでマルチキャスト通信を終了すると、該受信者端末のユーザ処理装置が前記認証サーバ処理装置に対してログアウト要求を行い、前記認証サーバ処理装置は該当ユーザの管理を終了することを特徴とする請求項１、請求項３又は請求項５に記載のマルチキャストシステム。

【請求項７】　マルチキャストデータを送信する送信者端末に設けられた第１のユーザ処理装置からのログイン要求を受理する手段と、

マルチキャストデータを受信する送信者端末に設けられた第２のユーザ処理装置からのログイン要求を受理する手段と、

送信者端末を有するユーザの個人情報が登録されたユーザ登録情報手段と、

を備える認証サーバ端末であって、

前記認証サーバ処理装置からログインを許可された送信者端末はマルチキャストデータを暗号化して送信し、

前記認証サーバ処理装置から予めユーザ登録情報手段にユーザとして登録された受信者端末は、ログインを許可されると共にマルチキャストデータを受信することを特徴とする認証サーバ端末。

【請求項８】　送信者端末を有するユーザの個人情報を登録し、

マルチキャストデータを送信する送信者端末からのログイン要求を受理し、

ログインを許可された送信者端末はマルチキャストデータを暗号化して送信し

マルチキャストデータを受信する送信者端末からのログイン要求を受理し、

前記認証サーバ処理装置から予めユーザ登録情報手段にユーザとして登録された受信者端末は、ログインを許可されると共にマルチキャストデータを受信することを特徴とするマルチキャスト受信者端末管理方法。

【請求項９】　送信者端末を有するユーザの個人情報を登録するステップと

マルチキャストデータを送信する送信者端末からのログイン要求を受理するステップと、

ログインを許可された送信者端末はマルチキャストデータを暗号化して送信するステップと、

マルチキャストデータを受信する送信者端末からのログイン要求を受理するステップと、

前記認証サーバ処理装置から予めユーザ登録情報手段にユーザとして登録された受信者端末は、ログインを許可されると共にマルチキャストデータを受信するステップと、

を有するマルチキャスト受信者端末管理方法のプログラムがコンピュータの利用可能な状態で記録された記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、マルチキャストによるデータ通信に関し、特に指定された認証サーバで参加者を個別認証することにより参加者を特定する構成に関する。

【０００２】

【従来の技術】

マルチキャストは、ユニキャストとブロードキャストの概念を総合したものである。つまり、マルチキャストデータが特定のホストに送られたり（ユニキャスト）、ネットワーク上の全ホストに送られる（ブロードキャスト）のではなく、任意の数のホストにデータパケットが同時に送られる。送信者はマルチキャストグループアドレスにデータを送り、そのデータの受信を希望する者は誰でも受信可能であることは既知である。また、暗号化を使用するデータストリーム保護方法は公知であり、送信者が受信者側での解読のためにデータパケットを暗号化するものである。

【０００３】

これは一般的に共通鍵暗号化技術を使用する。従来のマルチキャストにおけるデータフロー保護技術の一例が、特開平11-027252号公報と特開平11-127197号公

報に記載されている。特開平11-027252号公報では、鍵の扱いとして、データの暗号／復号に使用する鍵（公開鍵／秘密鍵）を鍵管理装置に保管する構成になっていると共に、マルチキャスト技術は復号鍵の配布に利用する構成が開示されている。特開平11-127197号公報では、鍵の扱いとしてユーザ認証に使用する鍵（共用キー／専用キー）はすべてドメインネームサーバまたは認証機関に保管する構成になっている。

また、特開平11-127197号公報に記載されている従来のマルチキャストにおけるデータフロー保護技術は、ユーザがマルチキャストに参加要求を出すとマルチキャストルータがドメインネームサーバにインストールされた共用キーを検索し、ユーザが認証されるべきか否かを判断するルーティングエレメント制御である。これによって認証されないユーザのアクセスは遮断される。

【０００４】

【発明が解決しようとする課題】

しかし、特開平11-027252号公報記載の技術では、復号鍵を取得可能なユーザは不特定多数であり、復号鍵を持っていれば解除時刻後に暗号化データを解読することが可能であるという問題点があった。また、特開平11-027252号公報の技術では、暗号鍵を取得可能なユーザは送信を許可されたユーザのみで、危険なデータの送出を避けることができるが、復号鍵の取得が可能なユーザはルータ以下の不特定多数であり、復号鍵を持っていれば暗号化データを解読することが可能である。即ち、認証サーバに登録されたユーザでなくてもマルチキャストデータ送受信可能になるという課題があった。

【０００５】

さらに、マルチキャスト通信において、現在誰がマルチキャストデータを送受信しているのかわからず、ユーザ別の対応ができないという問題点がある。その理由は、ネットワーク上のホストはIGMP（Internet Group Management Protocol）を使ってグループメンバーシップ情報をローカルマルチキャストルータに知らせるが、その知らせを受けたマルチキャストルータはローカルマシンに必要なパケットだけ転送する。マルチキャストルータは、自分のサブネットにどのホスト・グループのパケットを流せばよいのかがわかればよいので、実際に誰が参加し

ているのか、また何人参加しているかは、管理者も参加者の誰にも知らされない。別の問題点は、重要なマルチキャストデータを盗まれたことに気づかないことである。参加者を確定できれば、マルチキャスト通信による放送・会議でユーザごとのメンテナンスが可能になる。

本発明は上述する課題を解決するもので、マルチキャストによるデータ通信において、指定された認証サーバで参加者を個別認証することにより参加者を特定できるマルチキャストシステムを提供することを目的とする。

【０００６】

【課題を解決するための手段】

上記課題を解決する本発明のマルチキャストシステムは、図１に示すように、マルチキャストにおける送信者端末１１０と受信者端末１３０、１４０の管理を行う認証サーバ処理装置１０１と、該認証サーバ処理装置に対するログインを行う第１のユーザ処理装置１１２を有し、マルチキャストデータを送信する送信者端末１１０と、該認証サーバ処理装置に対するログインを行う第２のユーザ処理装置１３２を有し、マルチキャストデータを受信する受信者端末１３０とを備えるものである。

【０００７】

好ましくは、送信者端末１１０はマルチキャストデータを送信する際に、ユーザ処理装置１１２から認証サーバ処理装置１０１に対してログイン要求を行い、認証サーバ処理装置１０１からログインを許可されると、マルチキャストデータを暗号化して送信する構成とするとよい。

【０００８】

また、受信者端末１３０のユーザは、認証サーバ処理装置１０１に登録されているユーザとする。受信者端末１３０はマルチキャストデータを受信する際に、ユーザ処理装置１３２から認証サーバ処理装置１０１に対してログイン要求を行い、認証サーバ処理装置１０１からログインを許可されると、認証サーバ処理装置１０１から渡された暗号鍵を用いてマルチキャストデータを復号化してアプリケーション１３１で正常に受信することができる。

【０００９】

また、受信者端末１４０のユーザは、認証サーバ処理装置１０１に登録されていないユーザとする。受信者端末１４０はマルチキャストデータを受信する際に、ユーザ処理装置１４２から認証サーバ処理装置１０１に対してログイン要求を行うが、登録されていないので認証サーバ処理装置１０１からログイン不許可となり暗号鍵は渡されない。したがってマルチキャストデータをアプリケーション１４１で正常に受信することができない。

【００１０】

また、暗号鍵を第３者に盗まれて解読されることを防ぐため、認証サーバ処理装置１０１は定期的に暗号鍵を生成し、ログイン時と同様に暗号鍵を受信者端末１３０へ配布する構成とすると良い。定期的に配布する暗号鍵をユーザ処理装置１３２が受け取らなかった場合は、既に受信者端末１３０がマルチキャスト通信を終了しているものとみなし、認証サーバ処理装置１０１にてログアウト処理を行う構成とすると、セキュリティの確保が図れる。

【００１１】

また、受信者端末１３０のアプリケーション１３１でマルチキャスト通信を終了すると、ユーザ処理装置１３２が認証サーバ処理装置１０１に対してログアウト要求を行い、認証サーバ処理装置１０１は該当ユーザの管理を終了する。

【００１２】

このようにして、認証サーバ処理装置１０１にはログイン・ログアウト処理によるユーザの認証履歴、定期的な暗号鍵の再送によるユーザの参加履歴が保存されるので、該当するマルチキャスト・グループの現在の参加者・参加人数を確定することができる。さらに、マルチキャストアドレスへのすべてのアクセスが履歴として残るので、不正なアクセス（未登録のユーザによるログインや同一ユーザの重複ログインなど）を発見することが可能になるセキュリティシステムである。なお、マルチキャストシステムはサブネットワーク１２０が複数あっても、無くても稼動する。

【００１３】

本発明の認証サーバ端末は、マルチキャストデータを送信する送信者端末に設けられた第１のユーザ処理装置からのログイン要求を受理する手段と、マルチキ

ャストデータを受信する送信者端末に設けられた第２のユーザ処理装置からのログイン要求を受理する手段と、送信者端末を有するユーザの個人情報が登録されたユーザ登録情報手段とを備える認証サーバ端末であって、前記認証サーバ処理装置からログインを許可された送信者端末はマルチキャストデータを暗号化して送信し、前記認証サーバ処理装置から予めユーザ登録情報手段にユーザとして登録された受信者端末は、ログインを許可されると共にマルチキャストデータを受信することを特徴とする構成としている。

【００１４】

本発明のマルチキャスト受信者端末管理方法は、送信者端末を有するユーザの個人情報を登録し、マルチキャストデータを送信する送信者端末からのログイン要求を受理し、ログインを許可された送信者端末はマルチキャストデータを暗号化して送信し、マルチキャストデータを受信する送信者端末からのログイン要求を受理し、前記認証サーバ処理装置から予めユーザ登録情報手段にユーザとして登録された受信者端末は、ログインを許可されると共にマルチキャストデータを受信する手順としている。なお、送信者端末を有するユーザの個人情報を登録するのと同様にして、受信者端末を有するユーザの個人情報を登録しても良い。送信者端末に受信機能を設け、受信者端末に送信機能を設けると、認証サーバでの認証方法は同じなので、送信者端末でもデータ受信可能であるし、受信者端末からデータ送信可能となる。

【００１５】

【発明の実施の形態】

以下、図面を用いて本発明の実施の形態を説明する。

図１を参照すると、本発明のマルチキャストにおける参加者管理セキュリティシステムの一実施例は、認証サーバ端末１００と、送信者端末１１０、受信者端末１３０・１４０、インターネット/イントラネットなどのサブネットワーク１２０とから構成される。

【００１６】

認証サーバ端末１００の構成の詳細としては、ネットワークからの入力手段２００と、ネットワークへの出力手段２１０、ユーザ認証処理手段２２０、鍵管理

手段２３０、サーバ登録情報２４０、サーバ管理情報２５０とから構成される（図２）。送信者端末１１０の構成の詳細としては、ネットワークからの入力手段３００と、ネットワークへの出力手段３１０、入力データ処理手段３２０、データ暗号処理手段３３０、ユーザ登録情報３４０、鍵情報３５０、マルチキャスト通信可能なアプリケーション１１１とから構成される（図３）。受信者端末１３０・１４０の構成の詳細としては、ネットワークからの入力手段４００と、ネットワークへの出力手段４１０、入力データ処理手段４２０、データ復号処理手段４３０、ユーザ登録情報４４０、鍵情報４５０、マルチキャスト通信可能なアプリケーション１３１とから構成される（図４）。

【００１７】

ユーザ認証処理手段２２０は、ユーザ情報検索部２２１とユーザ認証部２２２を含む。鍵管理手段２３０は鍵更新制御部２３１と鍵生成部２３２を含む。入力データ処理手段３２０はデータ判別部３２１とユーザ情報作成部３２２を含む。データ暗号処理手段３３０は鍵管理部３３１と暗号データ作成部３３２を含む。入力データ処理手段４２０はデータ判別部４２１とユーザ情報作成部４２２を含む。データ暗号処理手段４３０は鍵管理部４３１と復号データ作成部４３２を含む。

【００１８】

これらの手段はそれぞれ概略つぎのように動作する。

サーバ登録情報２４０には、マルチキャスト通信する番組情報（マルチキャストアドレスやポート番号、暗号鍵の更新時間など）と番組の送受信を許可するユーザの情報（ユーザＩＤやユーザの公開鍵など）をあらかじめ登録する。番組とはマルチキャストによる放送や会議の主催者により定められたマルチキャストアドレスとポート番号を使用し、主催者により定められたマルチキャストデータ送信開始時間から送信終了時間までのマルチキャストデータ通信を指す。また、ユーザ登録情報３４０・４４０には、ユーザの個人情報（ユーザＩＤや参加予定の番組ＩＤ、認証サーバＩＤなど）をあらかじめ登録する。

【００１９】

認証サーバ処理装置１０１において、入力手段２００はユーザからのログイン

・ログアウト要求や暗号鍵の受理確認（ＡＣＫ）を受信し、出力手段２１０はユーザ認証処理手段２２０による認証結果や鍵管理手段２３０によって生成された暗号鍵を送信するための通信装置である。ログアウト要求を受けたサーバ認証処理装置１０１は暗号鍵の更新・再送を中止し、ユーザの管理を終了する。この一連のユーザ管理情報をサーバ管理情報２５０へ書き込む。

【００２０】

次に送信者端末１１０において、アプリケーション１１１から受け取ったマルチキャストデータと入力手段３００で受信した暗号鍵を入力データ処理手段３２０によって判別し、出力手段３１０はユーザ情報作成部３２２で作成したログイン・ログアウト要求情報やデータ暗号処理手段３３０による受理確認、暗号化したマルチキャストデータを送信する。

【００２１】

受信者端末１３０・１４０において、入力手段４００から受け取ったマルチキャストデータと暗号鍵を入力データ処理手段４２０によって判別し、出力手段４１０はユーザ情報作成部４２２で作成したログイン・ログアウト要求情報やデータ復号処理手段４３０による受理確認を送信する。復号データ作成部４３２によって復号化されたマルチキャストデータをアプリケーション１３１で表示する。

【００２２】

このように構成された装置の動作を次に説明する。次に、図２の構成図のフローチャート図５、図３・図４の構成図のフローチャート図６を参照して本実施例の全体の動作について詳細に説明する。

認証サーバにおいては、まずユーザの秘密鍵によるデジタル署名を用いて暗号化されたログイン要求情報を受け取ることからユーザ（参加者）の管理が始まる。ユーザのフローについては後述する。ログイン要求情報はユーザＩＤ、番組ＩＤのほかにタイムスタンプを含む（図５のステップＡ１）。ユーザ情報検索部２２１で、サーバ登録情報２４０に登録されているユーザＩＤから該当するユーザの公開鍵を検索しログイン要求情報を復号する。参加希望の番組に対してユーザＩＤが登録されているか確認する（ステップＡ２）。登録済みであれば認証し、認証結果をサーバ管理情報２５０に格納する。登録されていなければログインの

拒否を暗号化してユーザに通知し、この結果もサーバ管理情報２５０に格納する（ステップＡ３）。次に、鍵生成部２３２でサーバの秘密鍵でデジタル署名をした共通鍵をユーザの公開鍵で暗号化して送信し、次いでその共通鍵で暗号化した暗号鍵を送信する（ステップＡ４）。鍵の受理確認を受けた鍵更新制御部２３１はその結果をサーバ管理情報２５０に格納する。

【００２３】

待っても受理確認がこない場合は受信を終了したものとみなし、ログアウト処理しその情報をサーバ管理情報２５０に格納する。（ステップＡ５）。さらに、暗号鍵を不正に入手し利用されることを防ぐため、鍵更新制御部２３１において認証時刻から定期的に暗号鍵の再送を促す。番組が継続する場合は更新した暗号鍵をユーザへ配布する。番組が終了すると暗号鍵の配布も終了する（ステップＡ６）。また、ユーザからログアウト要求を受け取った場合は、該当ユーザへの更新した暗号鍵の配布を終了しログアウト処理を行い、その結果を暗号化してユーザへ送る。この結果はサーバ管理情報２５０に格納される（ステップＡ１）。

【００２４】

送信者がアプリケーション１１１を使ってマルチキャストデータを送信すると、まずデータ判別部３２１でそのマルチキャス通信が認証サーバによる認証処理が済んでいるか確認する（図６のステップＢ１）。認証処理がされていなければユーザ登録情報３４０からユーザＩＤ、番組ＩＤ（マルチキャストアドレスとポート番号）、認証サーバＩＤ（アドレスとポート番号）を取得しユーザ情報作成部３２２でログイン要求情報を作成し、事前に登録されていた認証サーバへ送信する（ステップＢ２）。認証結果を受け取り該当するマルチキャスト・グループへの通信を許可されると暗号化された暗号鍵を受け取る。認証されなかった場合はマルチキャストデータの送信を終了する（ステップＢ３）。暗号鍵は共通鍵暗号方式を用いて第３者による不正を保護している。復号するためには、ログイン後にサーバの秘密鍵によるデジタル署名を施した共通鍵を取得し、デジタル署名が正しい認証サーバのものであることを確認し、鍵管理部３３１で鍵情報３５０に管理する。

【００２５】

その後、配布された暗号鍵を保管している共通鍵で復号化し受理確認を認証サーバへ送信する（ステップＢ４）。暗号データ作成部３３２においてその暗号鍵を用いてマルチキャストデータを暗号化し暗号鍵のＩＤを付加して送信する（ステップＢ５）。認証後、継続してマルチキャストデータを送信する際、認証サーバから更新された暗号鍵を受信したら受理確認を送信する。更新された暗号鍵がなければ既存の暗号鍵を用いて暗号化する（ステップＢ６）。上記のフローをマルチキャストデータが継続するまで繰り返し、データ判別部３２１がアプリケーション１１１から送信終了の要求を受けると、ユーザ登録情報３４０からユーザＩＤ、番組ＩＤ（マルチキャストアドレスとポート番号）、認証サーバＩＤ（アドレスとポート番号）を取得し、ユーザ情報作成部３２２でログアウト要求情報を作成し認証サーバへ送信してマルチキャスト通信を終了する（ステップＢ７）。

【００２６】

受信者のフローは基本的に送信者と同形である。マルチキャストデータを受信すると、まずデータ判別部４２１でそのマルチキャスト通信が認証サーバによる認証処理が済んでいるか確認する（図６のステップＢ１）。認証処理がされていなければユーザ登録情報４４０からユーザＩＤ、番組ＩＤ（マルチキャストアドレスとポート番号）、認証サーバＩＤ（アドレスとポート番号）を取得しユーザ情報作成部４２２でログイン要求情報を作成し、事前に登録されていた認証サーバへ送信する（ステップＢ２）。認証結果を受け取り該当するマルチキャスト・グループへの通信を許可されると暗号化された暗号鍵を受け取る。認証されなかった場合はマルチキャストデータの受信を終了する（ステップＢ３）。暗号鍵は共通鍵暗号方式を用いて第３者による不正を保護している。復号するためには、ログイン後にサーバの秘密鍵によるデジタル署名を施した共通鍵を取得し、デジタル署名が正しい認証サーバのものであることを確認し、鍵管理部４３１により鍵情報４５０に管理する。

【００２７】

その後、保管している共通鍵で配布された暗号鍵を復号化し受理確認を認証サーバへ送信する（ステップＢ４）。復号データ作成部４３２において暗号鍵ＩＤ

から該当する暗号鍵を検索し、その暗号鍵でマルチキャストデータを復号化してアプリケーション１３１で受信する（ステップＢ５）。認証後、継続してマルチキャストデータを受信する際、認証サーバから更新された暗号鍵を受信したら受理確認を送信する。更新された暗号鍵がなければ既存の暗号鍵を用いて復号化する（ステップＢ６）。上記のフローをマルチキャストデータが継続するまで繰り返し、データ判別部４２１がアプリケーション１３１から受信終了の要求を受けると、ユーザ登録情報４４０からユーザＩＤ、番組ＩＤ（マルチキャストアドレスとポート番号）、認証サーバＩＤ（アドレスとポート番号）を取得し、ユーザ情報作成部４２２でログアウト要求情報を作成し認証サーバへ送信してマルチキャスト通信を終了する（ステップＢ７）。

【００２８】

次に、本発明の他の実施例について説明する。先の実施例において送信者が認証サーバを管理することができる場合、送信者端末上で認証サーバを実施する形態を設けることで、端末構成を簡素化でき、送信者用の暗号鍵をネットワーク上に流すことなく管理できるようになる。

図７を参照すると、本実施例は、認証サーバ兼送信者端末５００、受信者端末５１０、インターネット/イントラネットなどのサブネットワーク５２０とから構成される。認証サーバ兼送信者端末５００は認証サーバ処理装置５０１、マルチキャスト対応アプリケーション５０２、ユーザ処理装置５０３とから構成されている。受信者端末５１０はマルチキャスト対応アプリケーション５１１、ユーザ処理装置５１２とから構成されている。

【００２９】

認証サーバ兼送信者端末５００は前述した図２と図３を組み合わせた装置を有し、受信者端末５１０は図４と同一の装置を有する。本実施例におけるこれらの装置の動作の違いは、入力手段２００・３００及び出力手段２１０・３１０はネットワークとの通信装置であったことに対し、出力手段２１０の出力先が入力手段３００となり、ユーザ情報作成部３２２及び鍵管理部３３１による出力手段３１０の出力先が入力手段２００となるという点である。

【００３０】

本実施例の全体の動作については、認証サーバ兼送信者端末５００は前述した図５・図６の処理を並列に行い、受信者端末５１０は図６と同一の処理を行う。

【００３１】

【発明の効果】

以上説明したように、本発明によれば、第１の効果は、現在誰がマルチキャスト・グループに参加しているかを確定できることにある。認証サーバにおいて、ユーザＩＤにより各ユーザのログイン・ログアウト状況が管理されるため、送信者は受信してほしいユーザが存在していることを知ることができ、そのユーザの受信状況（受信開時間や受信終了時間）も知ることができるので、ユーザ管理に有効である。

【００３２】

第２の効果は、第３者の不正を防ぐことができることにある。重要なデータを流している場合は、そのデータが第３者に漏洩してしまうことを防ぐ必要がある。マルチキャストシステムはマルチキャスト・グループにアクセスしたすべてのユーザ情報が管理されるため、第３者の侵入にいち早く気づき対処することができる。

【図面の簡単な説明】

【図１】　本発明の一実施の形態を説明する構成ブロック図である。

【図２】　認証サーバ端末の詳細な構成ブロック図である。

【図３】　送信者端末の詳細な構成ブロック図である。

【図４】　受信者端末の詳細な構成ブロック図である。

【図５】　認証サーバ端末の動作を説明するフローチャートである。

【図６】　送信者端末並びに受信者端末の動作を説明するフローチャートである。

【図７】　本発明の第２の実施の形態を説明する構成ブロック図である。

【符号の説明】

１００　認証サーバ端末

１０１　認証サーバ処理装置

１１０　送信者端末

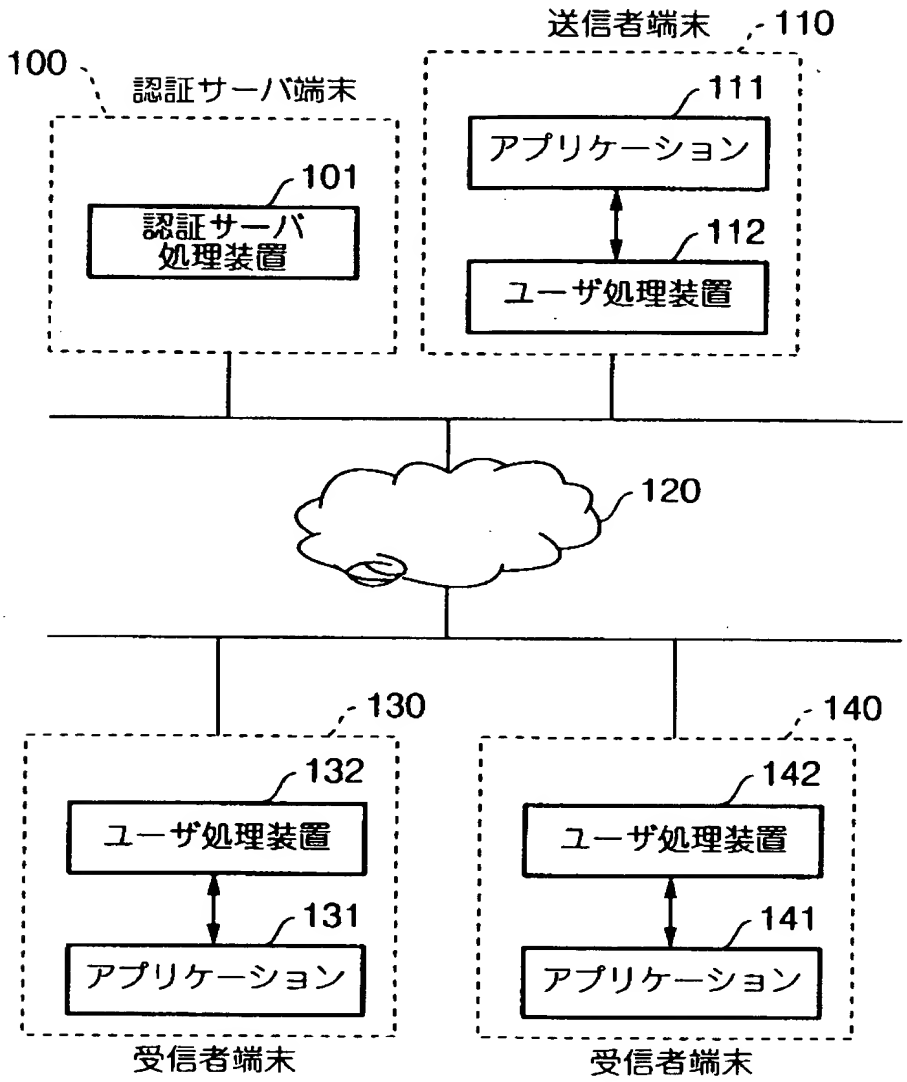
１２０　サブネットワーク

１３０　受信者端末

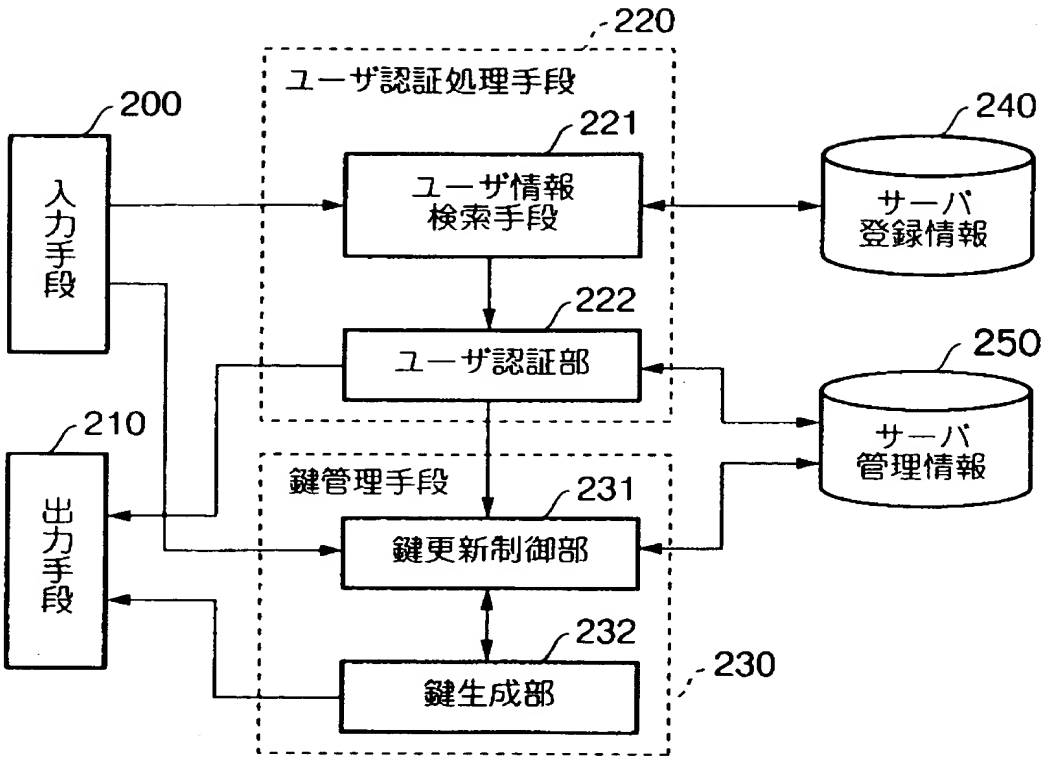
１４０　受信者端末

【書類名】　　図面

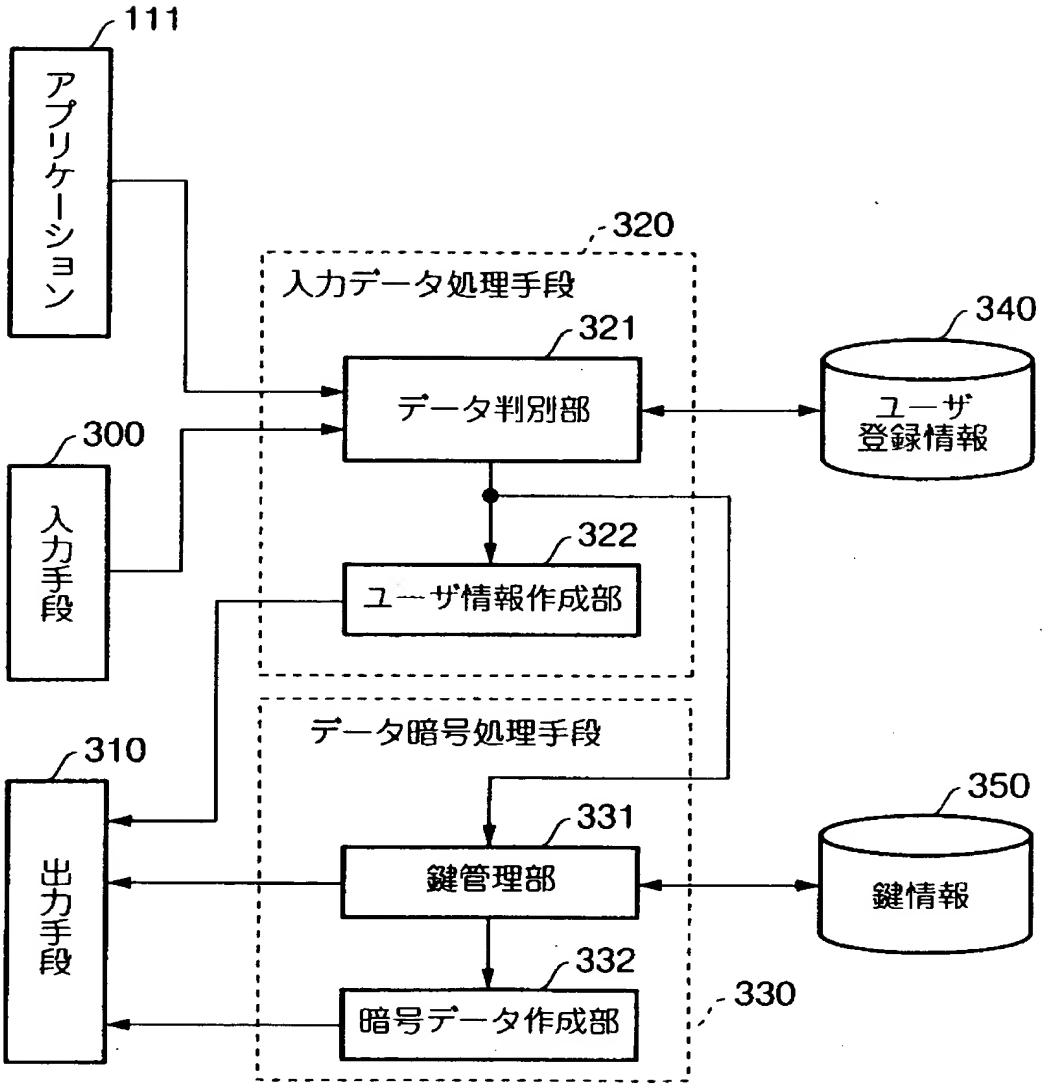
【図１】


送信者端末
110
100
認証サーバ端末
111
アプリケーション
101
認証サーバ
処理装置
112
ユーザ処理装置
120
130
140
132
ユーザ処理装置
142
ユーザ処理装置
131
アプリケーション
141
アプリケーション
受信者端末
受信者端末

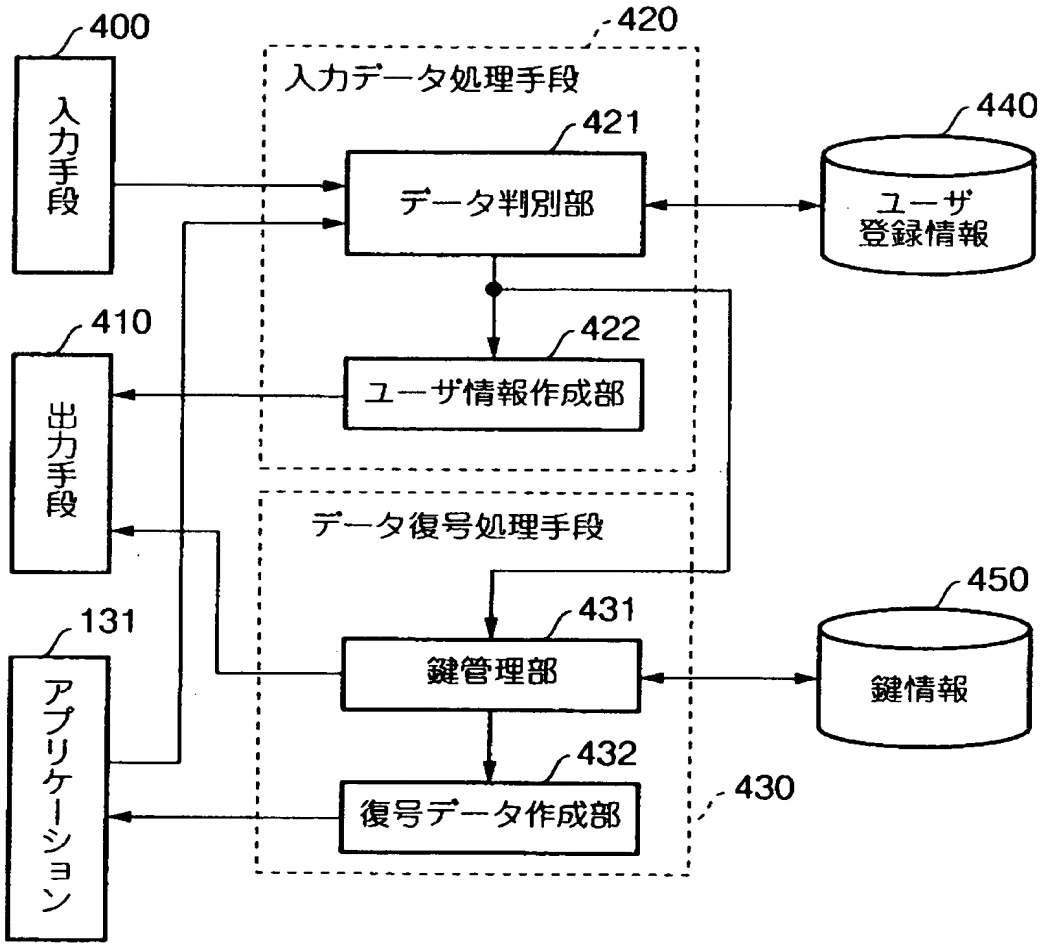
【図２】


220
ユーザ認証処理手段
200
入力手段
221
ユーザ情報検索手段
240
サーバ登録情報
222
ユーザ認証部
250
サーバ管理情報
210
出力手段
鍵管理手段
231
鍵更新制御部
232
鍵生成部
230

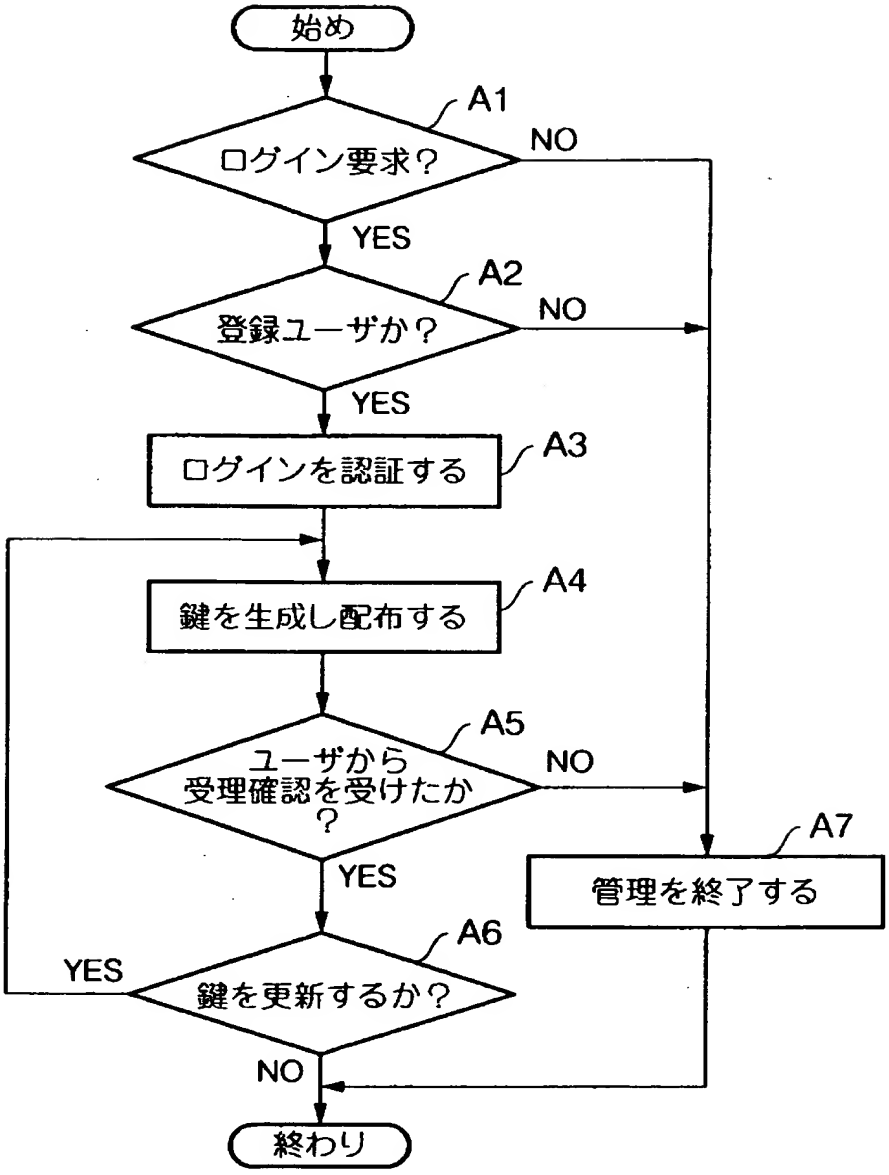
【図３】


111
アプリケーション
320
入力データ処理手段
340
321
データ判別部
ユーザ
登録情報
300
入力手段
322
ユーザ情報作成部
データ暗号処理手段
310
350
331
出力手段
鍵管理部
鍵情報
332
330
暗号データ作成部

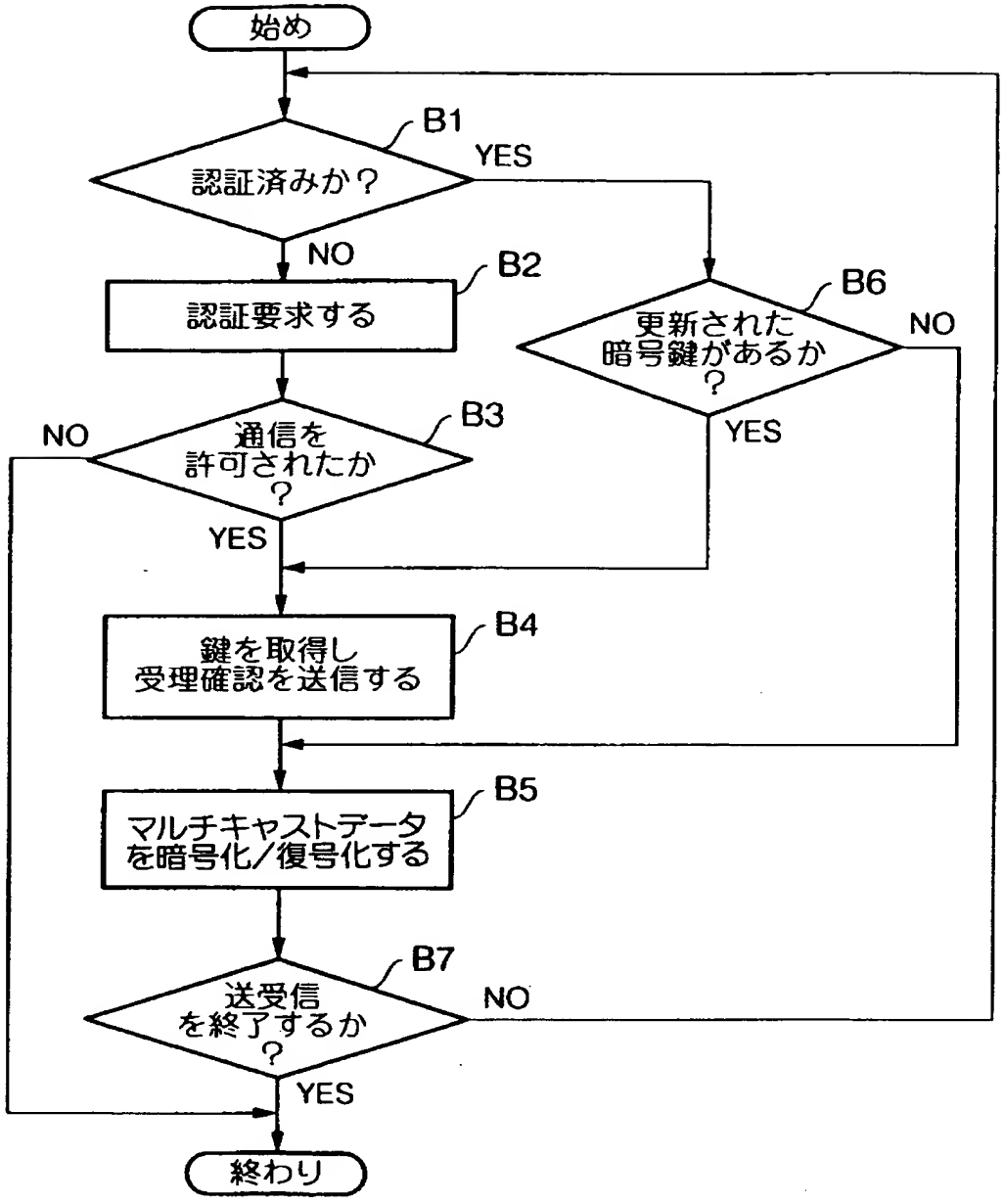
【図４】


400
入力手段
420
入力データ処理手段
421
データ判別部
440
ユーザ
登録情報
410
出力手段
422
ユーザ情報作成部
データ復号処理手段
450
131
アプリケーション
431
鍵管理部
鍵情報
432
復号データ作成部
430

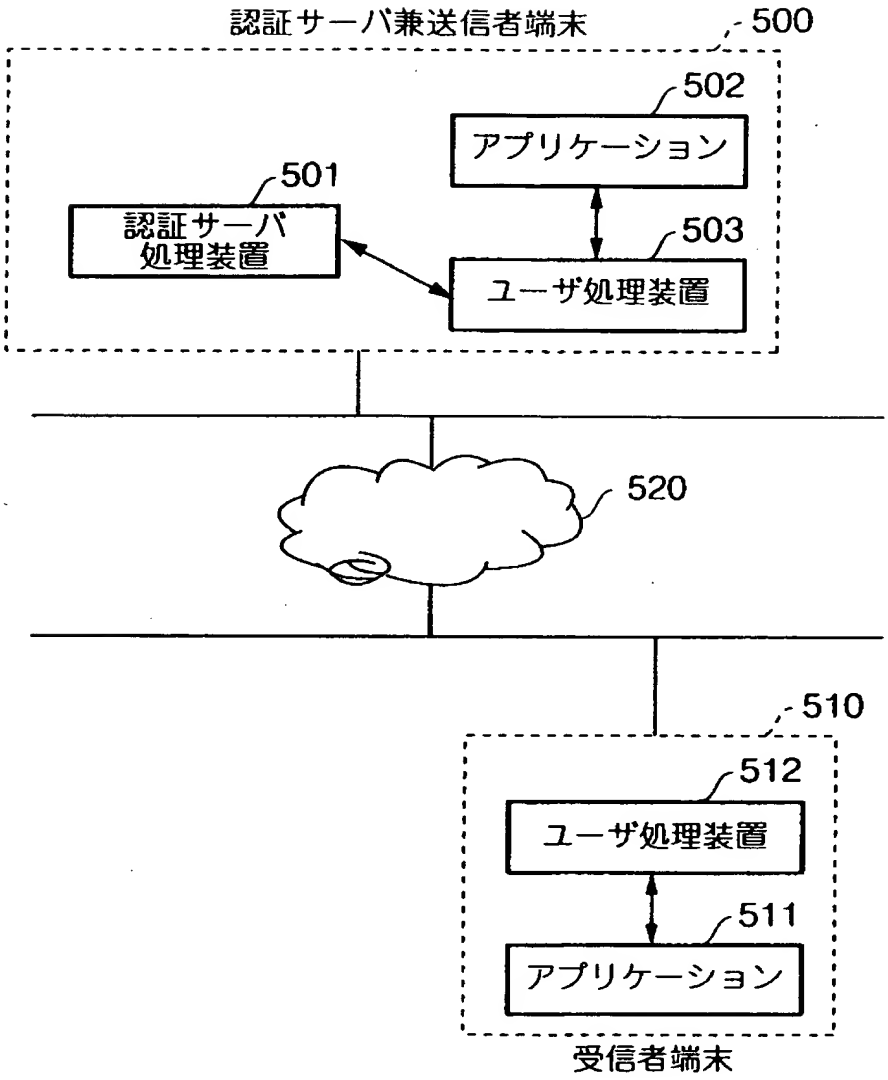
【図５】


始め
A1
ログイン要求？
NO
YES
A2
登録ユーザか？
NO
YES
ログインを認証する
A3
鍵を生成し配布する
A4
A5
ユーザから
受理確認を受けたか
？
NO
YES
A7
管理を終了する
A6
YES
鍵を更新するか？
NO
終わり

【図６】


始め
B1
認証済みか？
YES
NO
B2
認証要求する
B6
更新された
暗号鍵があるか
？
NO
YES
B3
通信を
許可されたか
？
NO
YES
B4
鍵を取得し
受理確認を送信する
B5
マルチキャストデータ
を暗号化／復号化する
B7
送受信
を終了するか
？
NO
YES
終わり

【図７】


認証サーバ兼送信者端末
500
502
アプリケーション
501
認証サーバ
処理装置
503
ユーザ処理装置
520
510
512
ユーザ処理装置
511
アプリケーション
受信者端末

【書類名】　　要約書

【要約】

【課題】　マルチキャストによるデータ通信において、指定された認証サーバで参加者を個別認証することにより参加者を特定できるマルチキャストシステムを提供する。

【解決手段】　本発明のマルチキャストシステムは、マルチキャストにおける送信者端末１１０と受信者端末１３０、１４０の管理を行う認証サーバ処理装置１０１と、該認証サーバ処理装置に対するログインを行う第１のユーザ処理装置１１２を有し、マルチキャストデータを送信する送信者端末１１０と、該認証サーバ処理装置に対するログインを行う第２のユーザ処理装置１３２を有し、マルチキャストデータを受信する受信者端末１３０とを備えるものである。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２０００－０７３０６４
受付番号	５００００３１２８３４
書類名	特許願
担当官	濱谷　よし子　　１６１４
作成日	平成１２年　３月２３日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000004237
【住所又は居所】	東京都港区芝五丁目７番１号
【氏名又は名称】	日本電気株式会社

【代理人】　申請人

【識別番号】	100108578
【住所又は居所】	東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】	高橋　詔男

【代理人】

【識別番号】	100064908
【住所又は居所】	東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】	志賀　正武

【選任した代理人】

【識別番号】	100101465
【住所又は居所】	東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】	青山　正和

【選任した代理人】

【識別番号】	100108453
【住所又は居所】	東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】	村山　靖彦

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社